UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A grey iPhone located in evidence at 5441 Watson Dr SE, Albuquerque, NM 87106

Case No. 24MR2332

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated by reference herein.

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. 846	Attempted Distribution of more than 100 grams of heroin

The application is based on these facts:

See attached affidavit, incorporated by reference herein and approved by AUSA Elaine Ramirez.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Gavin Hayes, HSI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephonically sworn and electronically signed *(specify reliable electronic means)*.

Date: December 20, 2024

Judge's signature

City and state: Albuquerque, New Mexico

Magistrate Judge Laura Fashing

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Gavin Hayes, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a one grey-colored Apple iPhone cellular telephone (referred to herein as the "Device") which is currently in law enforcement possession and described in Attachment A—and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations (HSI) and have been since April 4, 2024. As such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am empowered by law to conduct investigations and to make arrests for criminal offenses, to include those enumerated in 18 U.S.C. § 2516.

3. I have completed the Criminal Investigators Training Program (CITP) and Homeland Security Investigations Special Agent Training (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. These training programs included topics such as constitutional law, customs and immigration law, civil and criminal forfeiture, narcotics investigations, financial investigations, physical and electronic evidence, investigative methods, and more.

4. Prior to my tenure as a Special Agent, I was a sworn law enforcement officer employed by the city of Greensboro, North Carolina. I served in that position for over six years, during which I was primarily assigned to the patrol bureau. My primary responsibilities were responding to 911 calls and investigating violations of criminal law. I investigated and assisted

with investigating hundreds of felony and misdemeanor violent crimes, drug offenses, weapon violations, fraud offenses, impaired driving offenses, and more. I regularly established probable cause for warrantless arrests, arrest warrants, and search and seizure warrants for the aforementioned crimes.

5. My training as a Greensboro Police Officer included attending the Greensboro Police Academy, which included North Carolina's Basic Law Enforcement Training (BLET) program. Covered topics included constitutional law, criminal law, patrol duties, basic narcotics investigations, criminal investigations, basic interviewing, communication, and mental health awareness. Since completing the Greensboro Police Academy, I was certified by the State of North Carolina as a Chemical Analyst and as a Radar Operator. I received further specialized training in the areas of Fundamentals of the Investigative Process, Death and Violent Crime Scene Management, Standardized Field Sobriety Testing, Introduction to Drugged Driving, Drones for First Responders, and Roadside Interview and Detecting Deception.

6. Prior to my tenure as a Greensboro Police Officer, I received my education at Elon University in North Carolina. I received a Bachelor of Arts with majors in Public Health Studies and Policy Studies, and minors in Leadership Studies and Criminal Justice Studies.

7. In addition to my training and experience, I have developed information I believe to be reliable from additional sources including, but not limited to:

a. information provided by Special Agents ("SA"), Criminal Analysts ("CA") of the Department of Homeland Security, and other law enforcement officials (collectively referred to as "agents"), including oral and written reports that I have received directly or indirectly from said investigators;

b. Customs and Border Protection Officers ("CBPO"), their reports and analysis of illicit narcotics concealed within parcels intercepted during the international shipping process;

c. Results of physical surveillance conducted by agents during this investigation;

d. A review of telephone subscriber information;

e. Records from commercial databases;

f. A review of driver's license and automobile registration records; and

g. Records from the National Crime Information Center ("NCIC").

8. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

9. The property to be searched consists of one grey-colored Apple iPhone cellular telephone in a clear case currently stored in HSI Evidence Bag CS30483680 at 5441 Watson Dr. SE, Albuquerque, NM 87106. (referred to herein as the "Device"), which is further described in Attachment A.

10. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

DRUG TRAFFICKING AND CELLULAR DEVICES

11. Based upon my training and experience, and on my consultation with other law enforcement officers experienced in investigations regarding conspiracy to manufacture, distribute and possess with intent to distribute controlled substances, I have learned the following:

a. Those who possess illegal drugs for distribution often use electronic devices such as wireless or cellular telephones and smartphones. Such electronic devices are often used to communicate with coconspirators and customers through the telephone's standard capabilities to call and text, as well as through smartphone applications ("apps") such as WhatsApp, Snapchat, Pinger, Marco Polo and Facebook, which allow users to send and receive digital communications in various forms such as voice calls, text messages, image and video sharing, and live video conversations. Records of these communications, text messages, and contact lists are frequently retained and stored on those electronic devices and within those apps. Based upon my training, experience, and knowledge of this investigation, I believe that such evidence and information is likely to be found in the Device.

b. Individuals involved in the illegal trafficking of controlled substances often maintain documents, records, and other evidence of their transactions in a manner similar to the record keeping procedures of legitimate businesses. Even after the drugs are sold, documentary records are often maintained for long periods of time, even years, to memorialize past transactions, the status of accounts receivable and accounts payable, and the names and telephone numbers of suppliers, customers and co-conspirators. These records may be maintained on paper, in the form of business and personal ledgers and diaries, calendars, memoranda, pay/owe sheets, IOUs, miscellaneous notes, money orders, customer lists and telephone address books. These records can reflect names, addresses and/or telephone numbers of associates and co-conspirators, the sale and purchase of controlled substances including precursors, customer lists and amounts of

money owed to the trafficker by customers and by the trafficker to his/her suppliers. All such records can also be produced and/or stored on cellular telephones and evidence of these transactions is often contained within cellular phones.

c. Drug dealers often travel domestically and internationally to facilitate their trafficking. Evidence of foreign and domestic travel by persons engaged in illegal drug trafficking includes travel itineraries, airline tickets, hotel and gas receipts, and passports and visas and their contents. Many of these items are accessible via the internet and can be downloaded and saved on the computer or other media such as cellular phones.

d. Drug trafficking is a crime that necessarily involves at least two people – a buyer and a seller. Prior to engaging in the drug transaction, the buyer and seller must communicate and discuss the type of drug to be sold, the quantity, the price, and the location where the sale will take place. I know that drug dealers and their customers make use of cellular phones and smartphones to conduct these necessary communications.

e. Information stored in electronic form on cellular telephones can provide evidence of drug trafficking and the identity of associates. For example, numbers stored on cellular telephones (such as Caller ID lists reflecting recently received calls, speed dial lists of names and/or telephone numbers, and logs of outgoing and incoming calls) can provide evidence of who the drug dealer is calling, and thus the identity of associates.

f. Drug dealers often take, or cause to be taken, photographs and/or videos of themselves, their associates, their property, drug trafficking records, records of financial transactions involving drug trafficking proceeds, their drugs, and firearms. They usually

take these photographs and/or videos with their cellular phones and store them in those cellular phones.

g. I know that those engaged in drug trafficking have access to, and utilize, numerous cellular telephones, often at the same time in an effort to avoid law enforcement monitoring.

h. Electronic information can remain on computer storage media, such as within cellular phones, for an indefinite period of time. I am aware that even when a user attempts to delete records from computer storage media, the records may still exist and be recovered through computer forensic techniques.

PROBABLE CAUSE

Package Received from Mexico

12. On November 21, 2024, I received an email notification from a U.S. Customs and Border Protection ("CBP") officer at the Port of Cincinnati informing him that CBP inspectors had identified and seized an inbound parcel from the Republic of Mexico that contained approximately 324 grams of heroin.

13. The parcel in question (DHL Air Waybill ("AWB") Number 3066370882) had been shipped by "CLAUDIA ANDREA SANCHEZ MARTINEZ" at address "81475, Marte, 123, Salvador Alvarado, Salvado Alvarado Lvd. Lola Beltran #2555 Pte, Fraccionamiento Culiacan, 80054, SI, Mexico" and was addressed to "FERNANDO GARCIA SANCHEZ" at the address "5025 Central Ave NE, Albuquerque, NM 87108." The following was discovered after the documents associated with the seized parcel were examined:

a. The parcel arrived at the DHL shipment facility in Cincinnati, Ohio, in November 2024. The package had been manifested as "UB LIGHT LAMP AND ACRYLIC NAIL CASE."

b. An X-ray of the parcel revealed anomalies, which prompted officers to deploy a drug-detecting canine on the parcel. The canine alerted to the odor of illegal drugs inside the parcel.

14. As a result of the canine alert, officers searched the parcel. Inside, they found a brown substance concealed inside the "UB Lamp." The brown substance tested presumptively positive for the presence of heroin and weighed approximately 324 gross grams. Based on my training and experience, I know that 324 grams of heroin is consistent with distribution, not personal use.

15. On November 27, 2024, I received the parcel from CBP and secured it in the HSI Albuquerque evidence room. The parcel contained the "UB Light" and the heroin.

II. Controlled Delivery

16. On Wednesday, December 11, 2024, an Undercover Agent (UCA) with the United States Postal Investigative Service (USPIS) delivered a "Missed Delivery" notification to El Sinaloense, which is a business located at the address to which the parcel was addressed. The UCA spoke with an employee and instructed them to call the phone number on the notice for instructions on picking up the package.

17. On Friday, December 13, 2024, USPIS Inspector E. Byford was routed a phone call from (505) 544-0969, which she recognized as a number listed on the Bill of Lading for the parcel. Inspector Byford missed the first call, but soon received a second call from the number. Inspector

Byford answered this call, but the male-sounding caller hung up when they determined Inspector Byford did not speak Spanish.

18. On Friday, December 13, 2024, HSI Criminal Analyst ("CA") A. Licerio and I called (505) 544-0969 and posed as USPS employees. CA Licerio acted as a translator for this call. The male-sounding call recipient stated they had been trying to call for information about a package. I asked for the tracking number on the package. The call recipient provided the correct tracking number for the parcel. I said the package was for "Fernando" and asked the call recipient if that sounded correct. The caller answered that it was for "Fernando Garcia Sanchez," which matched the name to which the parcel was addressed. The call recipient agreed to meet at the Highland Post Office on Alvarado Drive in Albuquerque at 2 p.m. on Monday, December 16, 2024, to pick up the parcel.

19. On Monday, December 16, 2024, at around 3:30 p.m., Inspector Byford called (505) 544-0969 and explained to the male-sounding call recipient that they needed to pick up the package soon or it would be returned to the sender. The call recipient stated they were unable to personally pick up the package but would find someone to pick it up. Shortly thereafter, Inspector Byford received a call from (505) 544-0969, and the male-sounding caller stated they would personally pick up the package by 4:30 p.m. As this call was taking place, New Mexico State Police ("NMSP") Agents observed a person later identified as Juan Eduardo ESPARZA ASTORGA ("ESPARZA") exit the kitchen door of El Sinaloense while speaking on the phone.

20. NMSP Agents observed ESPARZA enter a brown 2014 Hyundai Elantra displaying New Mexico license plate BJRH92 and leave El Sinaloense.

21. Agents observed the same Hyundai enter the parking lot of the Highland Post Office located at 111 Alvarado Drive SE, Albuquerque, NM 87106. ESPARZA exited the Hyundai and looked underneath a black Nissan Titan before entering the post office.

22. Inspector Byford received a call from (505) 544-0969. The male-sounding caller stated they were at the post office, but the line was very long and they did not want to miss their package. Inspector Byford directed the caller to a different window. Inspector Byford then met with ESPARZA, who appeared visibly fidgety. ESPARZA then utilized his cell phone to pull up a picture of the missed delivery notification. He stated he was the person who had been calling Inspector Byford, and that the package belonged to him. ESPARZA then took possession of the parcel. (By this time, the heroin had been replaced with an inert substance.) ESPARZA then exited the post office and reentered the driver' s seat of the Hyundai with the parcel.

23. Agents attempted a vehicle stop on the Hyundai as it began to back out of its parking spot utilizing a "vehicle pin" maneuver, which involves making deliberate contact with the vehicle to surprise and disorient the driver. However, the Hyundai began moving before the pin could be completed. The Hyundai then backed into a stationary unmarked law enforcement vehicle which had activated its sirens. Other law enforcement vehicles, including two marked NMSP vehicles, began to surround the Hyundai with emergency lights activated. However, the Hyundai was able to escape containment by accelerating rapidly and turning. The Hyundai accelerated into the employee parking lot and began maneuvering recklessly by conducting abrupt braking maneuvers, a rapid U-turn, and accelerating rapidly enough that its tires squealed.

24. The Hyundai escaped the USPS parking lot and accelerated northbound on Alvarado Drive while continuing to drive recklessly. Specifically, the Hyundai failed to stop at

the red light at the intersection of Alvarado Drive and Central Avenue, causing a collision with another motor vehicle, which contained a family. There were no injuries as a result of this collision.

25. The Hyundai continued to accelerate rapidly as it traveled westbound on Central Avenue, causing law enforcement agents to briefly lose sight of the vehicle. Within less than five minutes, an unidentified bystander signaled to a marked NMSP unit that the suspect vehicle had turned northbound on Quincy Street NE, and the NMSP Agent located the Hyundai abandoned near the intersection of Quincy Street and Copper Avenue. Other NMSP Agents located ESPARZA running near the intersection of Copper Avenue and Manzano Street NE, about two blocks away from where the Hyundai was located. ESPARZA was detained without further incident. A search of ESPARZA's person incident to arrest located identity documents and the keys to the Hyundai

26. I conducted a probable cause search of the Hyundai. As I opened the unlocked door, I heard a phone ringing. I located the Device in question on the driver's floorboard and was able to put it in airplane mode before securing it in evidence bag CS30483680.

27. Based on the events described above, there is probable cause to believe that the Device will contain evidence of ESPARZA's drug trafficking activities, specifically violations of 21 U.S.C. § 846.

28. The Device is currently in the lawful possession of Homeland Security Investigations. They came into HSI's possession upon the arrest of ESPARZA on December 16, 2024, after which the grey-colored iPhone was located on the front passenger seat of the vehicle which ESPARZA was driving.

29. The Device is currently in storage at the Homeland Security Investigations office at 5441 Watson Dr SE, Albuquerque, NM 87106. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

TECHNICAL TERMS

30. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets,

and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

31. Based on my training, experience, and research, I know that the Device has capabilities that allows it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

35. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices

produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices

cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, if a locked device is equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

36. Based on the foregoing, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe ESPARZA's fingers (including thumbs) to the fingerprint scanner of the Device; (2) hold the Device in front of ESPARZA's face and activate the facial recognition feature, for the purpose of attempting to unlock the Device in order to search its contents as authorized by this warrant.

37. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

38. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachments A to seek the items described in Attachment B.

39. The affidavit has been reviewed by AUSA Elaine Ramirez.

Respectfully submitted,

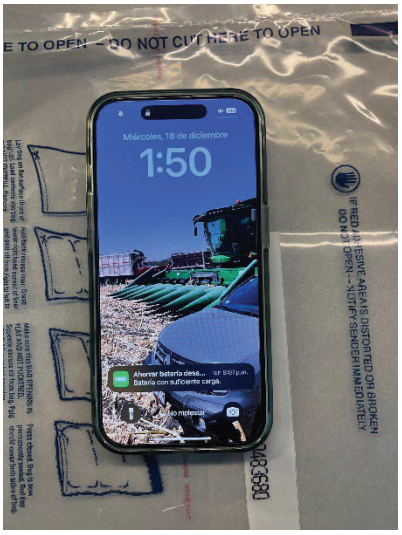
Gavin Hayes
Special Agent
Homeland Security Investigations

Sworn telephonically and signed electronically on December 20, 2024.

Honorable Laura Fashing
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a grey-color Apple iPhone currently in the custody of HSI in evidence bag CS30483680. It is in a clear case with the word "iHome" near the bottom. It does not display any identifying exterior markings. Photographs of the device are included below:



This warrant authorizes the forensic examination of this device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and information on the Device described in Attachment A that relate to violations of 21 U.S.C. §§ 841 and 846, from **November 20, 2024 to the date of the search,** including:

a. data and information identifying co-conspirators, customers, and suppliers;

b. communications between co-conspirators, customers, and suppliers;

c. data and information regarding the types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

d. data and information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

e. photographs and/or videos of illegal drugs, co-conspirators, drug trafficking records and/or records of drug trafficking transactions, and/or firearms;

f. financial records or other information regarding the expenditure or disposition of proceeds from the distribution of controlled substances including all bank records, checks, credit card bills, account information, and other financial records; and

g. records of travel.

2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the Device described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who was in possession of the Device, to the fingerprint scanner of the device; (2) hold the Device in front of the face those same individual(s) and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.